Data Export Agreement

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

DATA EXPORTER [insert data exporter, i.e. customer legal entity]

Company:

Name (written out in full):

Position:

Address:

Authorised Signature .....

and

DATA IMPORTER

Company:	EVRY INDIA Pvt. Ltd.
Name (written out in full):	Rajnish Mohan
Position:	CEO
Address:	SEZ - Unit 1 and 2, 5th floor of 'E' Block, Tower-E Global Village, Mylasandra– Pattenegere Villages, Off Bangalore-Mysore Expressway RVCE Post Bangalore-560059, Karnataka, India

Authorised Signature .....

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Dated 16 October 2018

This Agreement is effective when signed by both parties.

1. DEFINITIONS

For the purposes of the Clauses:

(a) "personal data", "special categories of data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) "the data exporter" means the controller who transfers the personal data;

(c) "the data importer" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection;

(d) "the sub-processor" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) the applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) "technical and organisational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. DETAILS OF THE TRANSFER

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. THIRD-PARTY BENEFICIARY CLAUSE

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. OBLIGATIONS OF THE DATA EXPORTER

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. OBLIGATIONS OF THE DATA IMPORTER

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

  (ii) any accidental or unauthorised access; and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body

composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. LIABILITY

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. MEDIATION AND JURISDICTION

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. COOPERATION WITH SUPERVISORY AUTHORITIES

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. GOVERNING LAW

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Norway.

10. VARIATION OF THE CONTRACT

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. SUB-PROCESSING

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely Norway.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA-PROCESSING SERVICES

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is:

- [insert data exporter, i.e. customer legal entity]

Data importer

The DATA IMPORTER is:

EVRY INDIA, an EVRY Group company, is an established software services provider having over 19 years of experience, with a focus on Insurance & Healthcare, Banking & Financial Services, Retail, and ISVs (Independent Software Vendors). EVRY INDIA's clients include Fortune 1000 companies, ISVs and tech start-ups. EVRY INDIA has a global footprint with offices in the US, India and group offices in Europe, besides multiple offshore development centers in Bangalore and Chandigarh, India. EVRY INDIA's process and project maturity is very high with its offshore center being CMMI 5, PCMM 3, ISO 9001 and ISO 27001 certified.

EVRY INDIA provides integrated services across the entire life cycle of software development including application development and maintenance, QA, DW/BI and Enterprise Mobility, 24*7 Remote Infrastructure and Applications Operations. EVRY INDIA brings focus to realizing client objectives by using tailored tools and processes integrated with built-in engineering support groups. A customized governance model designed for distributed and multi-cultural teams makes EVRY INDIA a winning choice for its global clients.

Data subjects

The personal data transferred may concern the following categories of data subjects (please specify):

- *Employees of the Data Exporter*
- *Employees of the Data Exporters' customers*
- *Customers of the Data Exporter, such as consumers, business customer's contact person(s) and other representatives*
- *Customers (both consumer and business) of the Data Exporters' customers*
- *Suppliers of the Data Exporter*

Categories of data

The personal data transferred may concern the following categories of data (please specify):

Any and all personal data that DATA EXPORTER legally has registered regarding its customer, customer's customers, suppliers, employees or employees of customer.This may include, but is not limited to the following categories; personal data relating to the employment relationship such as, names, direct manager's name, organizational unit, role/title, phone number, work telephone, mobile phone number, work email address, work postal address, work visiting address, image depiction.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

We refer to the summary further down in this document and description in the DPA between Customer and EVRY.

Sensitive personal data? Feks:Health information of individuals, racial or ethnic origin, or political opinions, philosophical or religious belifs, the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act, sex life, trade union membership (GDPR/ the Norwegian Personal Data Act)

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The data importer is primarily engaged to work on, provide support in connection with and otherwise perform technical tasks in relation with the data exporter's information systems' infrastructure that contains personal data. Thus, in this work, the data importer may be exposed to some of the personal data present in the system, however, only necessary in order to provide the technical service.

DATA EXPORTER [insert data exporter, i.e. customer legal entity]

Company:

Name (written out in full):

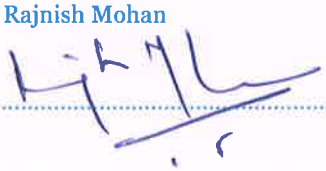
Authorised Signature .....

DATA IMPORTER

Company: EVRY INDIA Pvt. Ltd.

Name (written out in full): Rajnish Mohan

Authorised Signature .....



Summary of Appendix 1 and Appendix 2

The following descriptions are emphasized as the most relevant processing activities, categories of information and security measures, related to the services on software of Enterprise Content Management.

This is also described in the Data Processor Agreement (DPA) between EVRY and the Customer.

The processing activities are related to the following services:

- Installation and/or upgrading via online sessions or physical presence at Customer's location.
- Support for problem reported by the customer, via the customers and EVRY support system, further into data importer system for customer support.
- Troubleshooting on the Customers installation.
- Operation of the solution.

The following categories of personal information are processed:

- Contact information regarding customers support resources.
- Case documentation reported by the customer, in the support system, may contain information on the customer's customers, the clients. Potentially this documentation can contain sensitive personal information.

The following security measures are implemented in the value chain of the support service:

- Confidentiality Statements: The personnel who perform the services in the above roles have signed confidentiality statements.
- The data processor/data importer does not store data the customer exposes unless this is as part of an operating agreement with the customer.
- It is possible for the customer to delete documentation added as an attachment in the support system.
- The customer can also order support from EVRY consultants, in Norway, to ensure anonymization of information.
- The data importer does not have access to the customer's installation, any access is managed by the customer.

Clause 5 elaboration:

- EU Model Clauses is established between EVRY Norway ASA and EVRY India.
- EVRY India hold evidence of being GDPR compliant as a result of internal compliance project, both internal and as a part of EVRY.
- All consultants, working for EVRY, have compilated online training regarding GDPR and compliance.

Appendix 2
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. EVRY INDIA Pvt. Ltd : Ownership and Organization

EVRY INDIA Pvt. Ltd. (hereinafter referred to as EVRY INDIA) is a wholly owned subsidiary of EVRY (hereinafter referred to as "EVRY"). As such, EVRY INDIA is subject to compliance with EVRY Corporate Governance policies. Three EVRY top executives are members of the EVRY INDIA Board of Directors.

2. EVRY INDIA: Hiring procedures

EVRY INDIA herein confirms that their standard procedure for hiring new resources includes a background check conducted by their staff as well as signing the EVRY INDIA Non-disclosure agreement (NDA) and the EVRY INDIA Codes of Conduct document. The EVRY INDIA Codes of Conduct document is in compliance with the governing Codes of Conduct policy and documentation of EVRY.

EVRY INDIA herein also confirms that all of their resources participating in any engagement contracted via EVRY group, whether offshore, on-site or blended delivery, will sign both of the above mentioned documents. EVRY INDIA further confirms that the EVRY INDIA Codes of Conduct document has been distributed to all EVRY INDIA resources.

EVRY INDIA further informs that resources hired for international assignments where they will have to travel internationally must follow standard practice in India for acquiring a passport which includes a background check, also of the crime record, conducted by the Police Department.

EVRY INDIA confirms that all their resources participating in any engagement for DATA EXPORTER contracted via EVRY group for on-site, offshore or blended delivery will have acquired Indian passports and have therefore necessarily passed the Police Department's background check without incident.

3. EVRY INDIA and ISO27001

EVRY INDIA herein declares that they have built all of their IT processes using the guidelines provided in the ISO 27001 standard (also called BS7799 "Information Security Standard") EVRY INDIA is ISO 27001 and ISO 9001-2000 certified. EVRY INDIA´s ISO 9001-2000 and ISO 27001 certification was renewed in November 2013.

4. EVRY INDIA: Security aspects

4a. PHYSICAL ACCESS

Physical access to EVRY INDIA offices is restricted by security personnel. The offices are setup as open offices and resources enter the premises after swiping their employee cards or verifying them to a guard on duty. They are required to wear their employee cards at all times in the premises. CCTV is installed in EVRY INDIA offices and movement of people is tracked by security personnel round the clock to check for unauthorised entry.

4b. VISITORS

Visitors have to prove their identity upon arrival to the EVRY INDIA premises and obtain temporary visitors' cards at the reception. Visitors must also register their laptops at the security gate upon both check-in and check-out. They are accompanied by the host employee at all times inside the EVRY INDIA premises and are only allowed in the designated areas. They are also required to wear their visitors' cards at all times inside the EVRY INDIA premises.

4c. END OF EMPLOYMENT

When a resource leaves the company, the access rights to all the systems are revoked. The user account is blocked and all data is deleted from the laptop. The status in the company record is changed accordingly in the HR system and the employee card is destroyed. The resource has to get a clearance form signed from all the relevant departments, ensuring that all the exit steps are completed, before the resource leaves the EVRY INDIA office.

4d. SERVERS AND INFRASTRUCTURE

All servers utilized for DATA EXPORTER which contain data are located in secured Data Centers at EVRY, Norway, unless otherwise agreed between EVRY Norge AS and DATA EXPORTER .

Access to the databases and applications is strictly regulated based on need and approval by direct manager. Access to any application will be restricted to the module necessary to perform assigned tasks.

4e. ALL OFFSHORE WORKSTATIONS

At EVRY INDIA's offices, all the CD Drives and USB Ports are disabled in Desktops and servers accessible by resources engaged in tasks for DATA EXPORTER via EVRY Norge AS. Access to Printers from a Desktop or Server is also highly restricted.

Some of the Project Leads and senior Operations Staff will have laptops with CD Drives and USB Ports. These are resources who play a critical role in the team and whose help is required in case of emergencies or on call demands. Only such team members are allowed to take the laptop home. As this facility is provided to only senior and trusted team members and is restricted to a select few, the security risk arising out of this is very low.

4f. SECURE ACCESS TO ALL APPLICATIONS

All access to the applications will be provided according to EVRY's security requirements. Every resource working on any DATA EXPORTER application will be provided with separate user IDs and passwords with RSA security on COS VPN.

EVRY will provide a VDI environment to OFFSHORE resources to access DATA EXPORTER mainframe LPARS from an offshore location.

4g. LINK FROM EVRY INDIA TO OSLO

Network separation is achieved by segmenting the network. Network segmentation can be achieved easily in EVRY INDIA as the infrastructure supports network segmentation. EVRY INDIA provides network segmentation today to a number of their customers. They do this by building VLANs (Virtual LANS) wherein only machines belonging to the specific VLAN will have access to the information pertaining to that VLAN.

4h. HOME OFFICE ACCESS

Home access for resources to ServiceLAN is only allowed when proper role based access rights and log mechanisms are present and will then only be used for critical stand by operations. Such connections will use EVRY CISCO VPN and ServiceLan which is a secure connectivity solution from EVRY Norge AS to DATA EXPORTER applications. Security token can only be taken out of office premises, for selected resources, after personal permission has been approved by EVRY Norge AS.

4i. SECURITY AUDITS

EVRY Norge AS and DATA EXPORTER will have the right to audit the EVRY INDIA's implementation of DATA EXPORTER 's security requirements if stated in the agreement between EVRY Norge AS and DATA EXPORTER. During an audit, access shall be granted to relevant personnel, premises, documentation and other information relevant to processing of the data exporter's data.

Item	Appropriate corporate/legislative documents or procedures
1. EVRY India : Ownership and Organization	EVRY India Incorporation documents
2.EVRYIndia : Hiring procedures	EVRY India Guidelines for Hiring Process
4. EVRY India : Security aspects	EVRY IT Security Handbook and EVRY India Security Policy

4

4a. PHYSICAL ACCESS 5b. VISITORS	Section 6 EVRY India IT Security Policy Section 6.3 EVRY India IT Security Policy
4c. RESOURCES LEAVING EVRY India 4d. SERVERS AND INFRASTRUCTURE	EVRY India Employee Exit Process EVRY India Procedure for handling Desktop & Servers
4e. ALL OFFSHORE WORKSTATIONS DEDICATED TO DATA EXPORTER	EVRY India Procedure for handling Desktop & Servers
4f. SECURE ACCESS TO ALL APPLICATIONS DEDICATED TO DATA EXPORTER	Refer to EVRY Procedure
4h. HOME OFFICE ACCESS	Ref Section 8 of EVRY IndiaIT Policy (The home users are going to connect to EVRY network using VPN). Refer to EVRY procedure.
4i. SECURITY AUDITS	To be defined by EVRY AS in consultation with EVRY India

DATA EXPORTER [insert data exporter, i.e. customer legal entity]

Company:

Name (written out in full):

Authorised Signature .....

DATA IMPORTER

Company: EVRY INDIA Pvt. Ltd.

Name (written out in full): Rajnish Mohan

Authorised Signature .....

Appendix 3
to the Standard Contractual Clauses